

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 8月20日

出 願 番 号

Application Number:

平成11年特許願第233815号

出 願 人

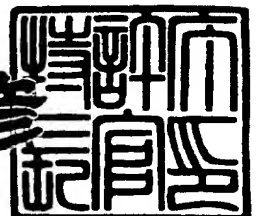
Applicant (s):

松下電器産業株式会社

2000年 6月 9日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3044856

【書類名】	特許願
【整理番号】	2022510372
【提出日】	平成11年 8月20日
【あて先】	特許庁長官殿
【国際特許分類】	H04L 9/32 H04L 12/14 H04L 9/00
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】	勝田 昇
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】	河田 浩嗣
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】	茨木 晋
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】	館林 誠
【発明者】	
【住所又は居所】	大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
【氏名】	原田 俊治
【特許出願人】	
【識別番号】	000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【プルーフの要否】 不要

【書類名】 明細書

【発明の名称】 データ再生装置および鍵記憶装置および情報埋め込み確認方法
および鍵使用履歴記録方法および透かし情報埋め込み装置およびその検出装置

【特許請求の範囲】

【請求項 1】 暗号化されたデータを復号する復号鍵記憶手段と前記復号鍵の読み取りを許可する読み取り許可手段と鍵の読み出し実績を記憶する読み出し履歴記憶手段を具備し、

前記復号鍵は、鍵の読み出し有効期間情報を含み、前記読み取り許可手段は、外部より読み取り要求時に要求時の時刻情報を含む鍵要求信号を受け取り、前記時刻情報の示す時刻が前記読み出し履歴情報の最も新しい時刻よりも後の時刻であることと鍵の読み出し有効期間内にあることを確認して読み取り許可を与えることを特徴とする鍵記憶装置。

【請求項 2】 さらに、履歴記憶手段は、履歴情報に加えてそのデータの改ざんが検出可能な改ざん検出コードを生成記録することを特徴とする請求項 1 記載の鍵記憶装置。

【請求項 3】 さらに、読み取り許可手段は、履歴情報につけられた改ざん検出コードにより、履歴情報に改ざんがないことを確認して読み取り許可を与えることを特徴とする請求項 2 記載の鍵記憶装置。

【請求項 4】 履歴記憶手段は、所定の記憶容量を持ち、読み取り許可手段は、履歴記憶手段に記憶された履歴情報が履歴情報記憶手段の記憶容量に達した時、鍵読み取りを不許可として制御することを特徴とする請求項 1 記載の鍵記憶装置。

【請求項 5】 復号鍵取得手段と前記取得した復号鍵に基づき入力データを解読処理する復号処理手段と復号されたデータに電子透かしを埋め込む電子透かし埋め込み手段と本装置の識別コードを記憶する機器識別コード記憶手段を具備し、

復号鍵取得手段は、復号鍵取得時、読み出し時点の鍵読み出し時刻を保持し、電子透かし埋め込み手段は、機器識別コードおよび前記鍵読み出し時刻を埋め込み情報として再生データに埋め込むことを特徴とするデータ再生装置。

【請求項 6】 さらに、復号鍵読み取り手段は、鍵を読み出す鍵記憶装置の識別番号を復号鍵とともに読み出すとともに保持し、電子透かし埋め込み手段は、鍵読み出し装置識別番号を埋め込み情報として埋め込むことを特徴とする請求項 5 記載のデータ再生装置。

【請求項 7】 さらに復号鍵取得手段は、読み出し時刻および機器識別コードを含む鍵読み出し履歴信号を生成し鍵記憶手段に伝送することを特徴とする請求項 5 記載のデータ再生装置。

【請求項 8】 暗号化されたデータの再生用鍵を記憶する鍵記憶手段と前記鍵記憶手段から再生用鍵データを読み出して再生処理するデータ再生手段からなり、データ再生手段と鍵記憶手段は、着脱可能な接続がなされ、鍵記憶手段は、データ再生手段が再生鍵を読み出したとき、データ再生装置の機器識別コードと読み出し時刻を含む鍵読み出し履歴を記録し、データ再生手段は、再生鍵に基づき再生する再生データに、再生鍵取得時刻および機器識別コードを透かし情報として埋め込むことを特徴とするデータ再生装置。

【請求項 9】 時刻情報および機器識別コードを透かし情報として埋め込んだデータ中より埋め込まれた透かし情報検出し、データへの情報埋め込み履歴データベースより前記検出処理で検出できた埋め込み情報と照合処理することを特徴とする埋め込み情報確認方法。

【請求項 10】 鍵の読み出し処理が行われた鍵読み出し時刻読み取り、最も近い以前の時刻に記録された時刻間を鍵未使用期間を意味するデータを記録し、次に前記鍵読み取り時刻を含む鍵読み取り情報を記録し、読み取られた鍵使用終了時、その終了時刻を記録することを特徴とする鍵使用履歴記録方法。

【請求項 11】 埋め込みパターンを各映像フレーム毎への埋め込み値列に変換する埋め込み列生成手段と各埋め込み列に基づき各フレームに情報を情報埋め込み手段からなり、埋め込み列生成手段は、埋め込みパターンを各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと埋め込みパターンを 1 ビットずつ複数フレームにわたって同じ値を埋め込むことにより埋め込みビット数の複数倍のフレーム数を用いて埋め込む長周期埋め込むパターンを混在させた埋め込みパターンを生成することを特徴とする透かし情報埋め込み

装置。

【請求項 1 2】 請求項 1 1 記載の透かし情報埋め込み装置により透かし情報を埋め込まれたデータから埋め込み情報を検出するものであって、各フレームから埋め込みパターンを検出するフレーム内埋め込み情報検出手段と前記フレーム内埋め込み手段が検出パターンより、短周期埋め込みされたビットに対応するパターンに基づき埋め込みパターンを算出する短周期埋め込みパターン検出手段と長周期埋め込みビットを参照して埋め込みパターンを算出する長周期埋め込みパターン検出手段からなる透かし情報検出装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、データへのアクセス権を有効期間ないだけ許すアクセス管理およびそのデータが著作物である場合の不正使用の検知や防止を実現可能なデータ再生装置および鍵記憶装置および埋め込み情報確認方法および鍵使用履歴記録方法に関する。

【 0 0 0 2 】

【従来の技術】

従来のデータ再生装置は、デジタルビデオディスクプレイヤー（DVDプレイヤー）などがある。これは、DVDビデオに格納されたデータを著作権保護対策を行わないような機器で再生できないように、ディスクにかかれるデータを暗号化して記録してあり、正規に鍵を付与されたプレイヤーのみ再生が可能になるものである。一般のDVDプレイヤーの場合、この再生用に機器に与えられた鍵は、固定的に与えられている。一方、映画の劇場への電子配信や航空機内のビデオサービスにおいては、劇場で公開される以前のものなどがあり、その再生できる期間を制御できるものが望まれている。このようなデータへのアクセスについて有効期限を設ける方法としては、鍵に有効期限を設け、鍵を利用する際に現在時刻を検出し、その時刻が有効期限内にあるかどうかによって鍵の利用を制御することで有効期間内だけ鍵を有効にすることができる。

【 0 0 0 3 】

また、データの再生に際して、その再生を行った機器の識別番号等を透かし情報として埋め込むことにより、再生データを不正にコピーして販売などをされた場合にその原因となった再生機器を突き止めることが考えられている。

【0004】

【発明が解決しようとする課題】

しかるに、従来の再生装置においては、有効期限を判定する際の正確な時刻を検出することが課題となっている。すなわち、現在時刻を検出する方法として再生装置内部に時計機能を持たせることが考えられるが、時計の誤差等を修正する機構を設けた場合、不正に時計を操作して再生装置内の時計を都合のよい時刻に変更されてしまう問題があった。同様に外部に時計を設けてそれを検出する場合もその時計への不正な操作が行われる問題があった。

【0005】

また、再生データに透かし情報を埋め込んだ場合、それを正しく検出する必要があるが、埋め込みデータが増えた場合、そのすべての情報を間違いなく検出することが困難になる問題があった。たとえば、映像信号中に機器の識別コードを埋め込んで追跡する場合、識別コードを正しく読まなくてはならないが、

映像信号に情報が埋め込まれていることがわからない程度に情報を埋め込める量は、少なく1フレーム内に埋め込みきれず数フレームに及んだ場合等には、そのうちの数フレームを抜き取るだけで正しく検出できない。また、検出結果が正しさを保証できる手段がなかった。

【0006】

以上のような問題に鑑み本発明の目的は、時刻情報を不正に操作して鍵有効期間外で鍵のアクセスによる不正なデータ再生を防止し、また不正なコピーに対してより高い追跡性を実現する再生装置および鍵記憶装置を提供することである。

【0007】

【課題を解決するための手段】

以上の課題を解決するために、本発明は、暗号化されたデータを復号する復号鍵記憶手段と前記復号鍵の読み取りを許可する読み取り許可手段と鍵の読み出し実績を記憶する読み出し履歴記憶手段を具備し、前記復号鍵は、鍵の読み出し有

効期間情報を含み、前記読み取り許可手段は、外部より読み取り要求時に要求時の時刻情報を含む鍵要求信号を受け取り、前記時刻情報の示す時刻が前記読み出し履歴情報の最も新しい時刻よりも後の時刻であることと鍵の読み出し有効期間内にあることを確認して読み取り許可を与える鍵記憶装置の構成である。

【0008】

また、さらに履歴記憶手段は、履歴情報に加えてそのデータの改ざんが検出可能な改ざん検出コードを生成記録する鍵記憶装置の構成である。

【0009】

また、さらに、読み取り許可手段は、履歴情報につけられた改ざん検出コードにより、履歴情報に改ざんがないことを確認して読み取り許可を与える鍵記憶装置の構成である。

【0010】

また、履歴記憶手段は、所定の記憶容量を持ち、読み取り許可手段は、履歴記憶手段に記憶された履歴情報が履歴情報記憶手段の記憶容量に達した時、鍵読み取りを不許可として制御する鍵記憶装置の構成である。

【0011】

また、復号鍵取得手段と前記取得した復号鍵に基づき入力データを解読処理する復号処理手段と復号されたデータに電子透かしを埋め込む電子透かし埋め込み手段と本装置の識別コードを記憶する機器識別コード記憶手段を具備し、復号鍵取得手段は、復号鍵取得時、読み出し時点の鍵読み出し時刻を保持し、電子透かし埋め込み手段は、機器識別コードおよび前記鍵読み出し時刻を埋め込み情報として再生データに埋め込むデータ再生装置の構成である。

【0012】

さらに、復号鍵読み取り手段は、鍵を読み出す鍵記憶装置の識別番号を復号鍵とともに読み出すとともに保持し、電子透かし埋め込み手段は、鍵読み出し装置識別番号を埋め込み情報として埋め込むデータ再生装置の構成である。

【0013】

さらに復号鍵取得手段は、読み出し時刻および機器識別コードを含む鍵読み出し履歴信号を生成し鍵記憶手段に伝送するデータ再生装置の構成である。

【0014】

また、暗号化されたデータの再生用鍵を記憶する鍵記憶手段と前記鍵記憶手段から再生用鍵データを読み出して再生処理するデータ再生手段からなり、データ再生手段と鍵記憶手段は、着脱可能な接続がなされ、鍵記憶手段は、データ再生手段が再生鍵を読み出したとき、データ再生装置の機器識別コードと読み出し時刻を含む鍵読み出し履歴を記録し、データ再生手段は、再生鍵に基づき再生する再生データに、再生鍵取得時刻および機器識別コードを透かし情報として埋め込むデータ再生装置の構成である。

【0015】

時刻情報および機器識別コードを透かし情報として埋め込んだデータ中より埋め込まれた透かし情報検出し、データへの情報埋め込み履歴データベースより前記検出処理で検出できた埋め込み情報と照合処理する埋め込み情報確認方法である。

【0016】

また、鍵の読み出し処理が行われた鍵読み出し時刻読み取り、最も近い以前の時刻に記録された時刻間を鍵未使用期間を意味するデータを記録し、次に前記鍵読み取り時刻を含む鍵読み取り情報を記録し、読み取られた鍵使用終了時、その終了時刻を記録する鍵使用履歴記録方法である。

【0017】

また、埋め込みパターンを各映像フレーム毎への埋め込み値列に変換する埋め込み列生成手段と各埋め込み列に基づき各フレームに情報を情報埋め込み手段からなり、埋め込み列生成手段は、埋め込みパターンを各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと埋め込みパターンを1ビットずつ複数フレームにわたって同じ値を埋め込むことにより埋め込みビット数の複数倍のフレーム数を用いて埋め込む長周期埋め込むパターンを混在させた埋め込みパターンを生成する透かし情報埋め込み装置の構成である。

【0018】

また、透かし情報を埋め込まれたデータから埋め込み情報を検出するものであって、各フレームから埋め込みパターンを検出するフレーム内埋め込み情報検出

手段と前記フレーム内埋め込み手段が検出パターンより、短周期埋め込みされたビットに対応するパターンに基づき埋め込みパターンを算出する短周期埋め込みパターン検出手段と長周期埋め込みビットを参照して埋め込みパターンを算出する長周期埋め込みパターン検出手段からなる透かし情報検出装置もの構成である。

【 0 0 1 9 】

【 発明の実施の形態 】

以下、本発明の実施の形態について、添付図面を参照して説明する。

【 0 0 2 0 】

（実施の形態 1）

図 1 は、本発明の実施の形態 1 のデータ再生装置および鍵記憶装置を含むシステムの構成図である。図 1 において、1 は、鍵の生成などを行う鍵管理部、2 は、鍵管理部 1 が生成した鍵を記憶する鍵記憶装置で、鍵管理部で生成した再生装置鍵記憶部 3 とその有効期間記憶部 4、鍵の読み取り履歴記憶部 5 および鍵記憶装置識別コード記憶手段 6 からなり、7 は、データ再生装置であり、データ再生装置識別コード記憶部 8 と鍵複号処理部 9、再生処理部 10 および電子透かし埋め込み処理部 11 からなり、12 は、時計、13 は、暗号化データおよびその暗号化鍵を再生装置鍵で暗号化されたものが記憶された記録メディア（たとえば、DVD）、14 は、鍵暗号化手段、15 は、データ暗号化手段である。

【 0 0 2 1 】

以上のような構成において以下にその動作を説明する。鍵管理部 1 は、データ再生装置毎の再生装置鍵を生成し、鍵記憶装置 2 の再生装置鍵記憶部 3 とその有効期間記憶部 4 へ記録する。また、映画などのコンテンツデータを記録メディアに書き込み者へ再生装置鍵およびその有効期間を送る。その再生装置鍵は、鍵暗号化手段 14 へ入力される。コンテンツデータは、コンテンツ鍵で並データ暗号化処理部 15 で暗号化され記録メディア 13 に記録される。また、この時のコンテンツ鍵を再生装置鍵を用いて暗号化処理手段 14 で暗号化したものを記録メディア 13 にあわせて記録する。以上のように、コンテンツデータをコンテンツ鍵で暗号化した暗号化コンテンツデータとそのコンテンツ鍵を再生装置鍵で暗号化

した暗号化コンテンツ鍵が記録された記録メディアが生成され、再生装置 7 へ送られる。これらの処理は、一般の DVD ビデオの映画タイトル等の生成において行われているため、処理の概略を示したが、複数の再生装置へ配布可能にするために、通常は、その配布先の再生装置鍵でコンテンツ鍵を暗号化したものを複数記憶させておく。

【0022】

図 1 に戻って、記録メディア 13 のデータを鍵記憶装置 2 およびデータ再生装置 7 で再生する処理を説明する。データ再生装置 7 は、記録メディア 13 を再生する場合、接続された鍵記憶装置 2 から再生装置鍵を読み取り、それを鍵復号処理部 9 に入力し、記録メディア 13 より暗号化コンテンツ鍵を読み出し鍵復号処理部 9 に入力して復号し、その復号されたコンテンツ鍵を再生処理部 10 へ入力する。再生処理部 10 は、暗号化コンテンツデータをコンテンツ鍵を用いて暗号解読したのち、そのデータの内容にしたがって再生処理する。たとえば、MPEG2 フォーマットで圧縮されたビデオデータの場合、MPEG2 デコーダ処理され、映像信号に再生される。データ再生装置 7 が、再生装置鍵を読み取る際、時計 12 より時刻情報を取得し、再生装置識別コードとともに時刻情報を鍵記憶装置 2 へ送る。この際、再生するコンテンツデータにコンテンツ識別情報がある場合は、コンテンツ識別情報も送る。鍵記憶装置 2 は、送信されてきた時刻情報と有効期間記憶部 4 の有効期間を比較し、有効期間内であれば再生装置鍵記憶部 3 内の再生装置鍵と鍵記憶装置識別コード記憶部 6 内の鍵記憶装置識別コードをデータ再生装置 7 へ送る。そして、データ再生装置 7 から送られたきた時刻情報、再生装置識別コード、コンテンツ識別コードを履歴情報として履歴情報記録部 5 に記録する。次に、データ再生装置 7 は、鍵読み取り時刻情報と再生装置識別コードおよび鍵記憶装置識別コードを埋め込み情報として電子透かし情報埋め込み処理部 11 で再生データに埋め込み処理する。

【0023】

鍵記憶装置 2 とデータ再生装置 7 間の処理の詳細を図 2 から図 6 を用いて説明する。図 2 は、鍵記憶装置 2 の構成図である。図 2 において、201 は、入出力インターフェイスでデータ再生装置 7 あるいは、鍵管理部 1 と接続される場合に

用いられ、202は、制御部、203は、履歴情報記憶部、204は、再生装置鍵記憶部、205は、有効期間記憶部、206は、鍵記憶部再生装置間鍵記憶部、207は、鍵記憶装置識別コード記憶部、208は、コンテンツ識別コード記憶部、209は、再生装置識別コード記憶部、210は時刻情報記憶部である。図3は、データ再生装置7の構成図である。図3において、301は、鍵記憶装置2との入出力インターフェイス部であり、図2の入出力インターフェイス部201と接続され、302は、制御部、303は、鍵記憶装置識別コード記憶部、304は、再生装置識別コード記憶部、305は、鍵取得時刻記憶部、306は、鍵復号処理部、307は、再生処理部、308は、電子透かし情報埋め込み処理部、309は、コンテンツ識別コード記憶部、310は、鍵記憶部再生装置間鍵記憶部である。

【0024】

以下動作を説明する。鍵記憶装置2とデータ再生装置7は、入出力インターフェイス201および301で接続される。たとえば、鍵記憶装置2は、スマートカードのようなCPU付きのメモリカードで実現でき、この場合ならメモリカード接点とICカードリーダーが入出力インターフェイス201、301にそれぞれ対応する。接続されると制御部202および302間の制御手順にしたがって鍵の読み取りが行われる。図4は、再生装置鍵の取得処理の処理手順の説明図である。同図において、401は、コンテンツ識別コード取得処理、402は、時刻情報取得処理、403は、鍵リクエスト送信処理、404は、最新読み取り時刻との比較処理、405は、鍵有効期間確認処理、406は、履歴書き込み処理、407は、鍵配送処理である。制御部202と302間の送信データは、鍵記憶部再生装置間鍵記憶部206および310にある共有されている鍵記憶部再生装置間鍵で暗号化通信される。暗号復号化処理は、制御部202および302でソフト的に行うことが可能である。まず、記録メディア13がデータ再生装置7にかけられたとき、制御部302は、記録メディア13内にあるコンテンツ識別コードを読み取りコンテンツ識別コード記憶部309に記憶する。次に時計12より、時刻情報取得402で時刻情報を読み出し、鍵取得時刻記憶部305に記憶する。次に、鍵リクエスト送信処理403で鍵をリクエストコマンドに鍵取得時刻

記憶部305の時刻情報と再生装置識別コード304内の再生装置識別コードおよびコンテンツ識別コード309内のコンテンツ識別コードをつけて送信する。次に、制御装置202は、コンテンツ識別コード記憶部208再生装置識別コード記憶部209、時刻情報記憶部210にそれぞれ送られてきた値を記憶して、最新読み取り時刻との比較処理404で履歴情報記憶部203の最新の時刻と時刻情報記憶部210の値を比べ、最新情報よりも時刻情報が以後の時刻を示していれば処理が成功し、もしそうでなければ、以後の処理を直ちに中止する。つぎに鍵有効期間確認処理405で、制御部202は、時刻情報210の時刻が有効期間205内に示された有効期間内にあれば、処理が成功したとし、そうでなければ以後の処理を直ちに中止する。そして、履歴書き込み処理407で、コンテンツ識別コード記憶部208、再生装置識別コード記憶部209、時刻情報記憶部210の情報を履歴情報として記憶する。ただし、履歴書き込むに失敗すれば、以後の処理を直ちに中止する。

【0025】

以上の3つの処理が成功すれば、鍵配送処理407で、制御部2は、再生装置鍵記憶部204内ので再生装置鍵を鍵記憶装置識別コード記憶部207の再生装置識別コードとともに制御部302に送信する。そして、履歴書き込み処理407で、コンテンツ識別コード記憶部208、再生装置識別コード記憶部209、時刻情報記憶部210の情報を履歴情報として記憶する。

【0026】

図5は、履歴情報の記録例であり、図6は、その記録処理手順の説明図である。図6において、601は、開始処理、602は、鍵を利用していない期間を記録する未使用期間記録処理、603は、開始時刻を記録する開始時刻記録処理、604は、鍵使用終了時刻記録処理である。

【0027】

以下処理を説明する。図5において、最初の1行目は、すでに書き込まれているものとする。これは、鍵の有効期間の開始時刻が書き込まれている。未使用期間記録処理602では、その時点で書き込まれている最終行の一番左の列の時刻情報を現在時刻の時間差を未使用時間として1列めに記録する。2列目には、最終

行の一番左の列の時刻情報を3列目は、現在時刻を記録する。そして、今書き込んだ行と一つ前の行のデータについての改ざん検出用のハッシュ処理を行い4列目に記録する。

【 0 0 2 8 】

次に、開始時刻記録処理 6 0 3 は、現在時刻を1列目に、2列目に再生装置識別コード、3列目にコンテンツ識別コードを記録し、さらに今書き込んだ行と一つ前の行のデータについての改ざん検出用のハッシュ処理を行い4列目に記録する。

【 0 0 2 9 】

次に、制御部 3 0 3 が取得した再生装置鍵の使用を終了したことを示す信号として時刻情報を送信したとき、制御部 2 2 は、鍵使用終了時刻記録処理を行う。これは、送られてきた終了時刻を1列目に、2列目に再生装置識別コード、3列目にコンテンツ識別コードを記録し、さらに今書き込んだ行と一つ前の行のデータについての改ざん検出用のハッシュ処理を行い4列目に記録する。

【 0 0 3 0 】

以上の処理により、履歴情報は、常に記録されるたびに直前の情報との改ざん検出コードでつながれるため、改ざん検出コードの生成方法が暴露されない限り、途中で不正な履歴を挟むと簡単にその位置が検出できる。そして記録去れるデータの最終行の1列めデータが最新の時刻情報であり、常にこの時刻よりも進んだ時刻が示されない限りられてきた値を記憶して、最新読み取り時刻との比較処理 4 0 4 で処理を中止されてしまうので、時刻情報を逆に進ませる不正を防止できる。また、鍵に取得時刻に加えて終了時刻まで記録した場合には、少なくともその再生時間分は、時刻を進ませることができるので時刻の不正を働いてもその再生できる時間は高々完全に連続再生している場合より長くはできない。また、履歴記憶部の容量を有限の値にしておけば、その記憶量いっぱい履歴が書き込まれるとそれ以上履歴が書き込めないで処理が不成功となり鍵配送されなくなるため、記憶容量によって鍵取得回数の上限を制限できる。

【 0 0 3 1 】

図 7 は、図 5 のように記録された履歴が電子透かし情報の読み出し処理に利用

する場合の説明図である。図7において、701は、不正に複製された記録メディア、702は、電子透かし情報検出装置、703は、再生装置識別コードによる検索検証処理、704は、鍵記憶装置識別コードによる検証処理、705は、鍵取得時刻情報による検証処理である。電子透かし情報検出処理702で検出された埋め込み情報は、不正者により改ざんされている可能性がある。すなわち、不正を働いたものは、埋め込み情報による追跡から逃れるために埋め込み情報の削除や改ざんを試みるのが想定される。その結果、埋め込み部分を抜き取る事による情報の欠損や、でたらめなデータの埋め込みによる改ざんへの試みによる一部のデータの誤検出が考えられる。そこで、埋め込まれた情報のどれか一つでも正しく検出されていた場合には、鍵記憶装置に貯えられた履歴を回収する事でできる履歴データベースを検索することで残りの情報を復元できる。再生装置識別コードによる検索検証処理703、鍵記憶装置識別コードによる検証処理704、鍵取得時刻情報による検証処理705でそれぞれの情報から残りの情報を復元できる。またこれらの情報をまとめて、それと最も相関性の高いものを履歴情報から見つける事でかなり高い確率で不正を行ったデータ再生装置や鍵記憶装置や犯行時刻等が推定できる。

【0032】

図8は、電子透かし情報埋め込み手段11あるいは308の構成とその検出装置の構成の説明図である。図8において801は、埋め込みシーケンス生成部、802は、映像1フレームに情報埋め込み処理する電子透かし埋め込み処理部、803は、短周期埋め込みパターン検出部、804は、長周期埋め込みパターン検出部、805は、電子透かし検出部である。以上の構成において以下にその動作を説明する。埋め込みパターンとして、機器識別コード、鍵記憶装置識別コードや時刻情報を含んだビットパターンが代入される。入力されたビットパターンは、埋め込みシーケンス生成部801で各映像フレームに埋め込むパターンの列に変換され、各フレーム毎に電子透かし埋め込み処理部802に送られる。埋め込みシーケンス生成部では、入力された埋め込みパターンを1フレーム当たり埋め込めるビット数に応じて分割して各フレームへの埋め込みパターンとする。たとえば、簡単のために埋め込みパターンが8バイトで1フレーム当たり4ビット

を埋め込み処理する場合、埋め込みパターンが“0 1 1 0 0 1 0 1 1 1 0 0 1 0 1 0”ならば、各フレームには、順に16進数で“6 5 c a”を最初の4フレームに埋め込む。次に、今の埋め込みパターンと同じフレーム数の映像に埋め込みパターンの第一ビットパターンである“0”を入力する。次に、先程入れたパターンと同じフレーム長間、埋め込みパターンの先頭ビット値を埋め込み値として埋め込む。すなわち、埋め込み値が0のときは、4フレーム間0を、1の場合は、4フレーム間16進数でF F F Fを出力する。次に再び最初に埋め込んだパターン“6 5 c a”を順に埋め込み、次に埋め込み値の第2のビットを埋め込む。以上のように、埋め込みパターンを順に埋め込み次にそれと同じ長さの期間内に1ビットだけ埋め込むことを順に繰り返す。すなわち、順に埋め込んだ短周期の埋め込みとそのビット数倍の長周期に繰り返す埋め込みパターン列を生成する。図9は、その埋め込み処理の結果、各フレームに埋め込まれるパターン列を説明した図である。電子透かし埋め込み処理部802では、各フレームごとに入力されるパターンにそって情報埋め込み処理して、埋め込み情報つきデータとする。検出の場合は、電子透かし情報検出部805で各フレーム毎の埋め込みパターンを検出する。本実施の形態では、原画像を参照画像として用いているが、参照画像なしで検出できる埋め込み方式の場合原画像を参照しなくてもよい。各フレームの埋め込みパターン検出結果は、短周期埋め込みパターン検出部803、長周期埋め込みパターン検出部804へ送られる。短周期埋め込みパターン検出部803は、短周期に埋め込まれたビット列部分の検出結果を繰り返し、比較し各ビットで最も出現回数が多い方のビット値として検出値とする。長周期埋め込みパターン検出部804は、各ビットの埋め込み期間内での検出結果、たとえば、図9における第5フレームから第8フレームまでが、すべて1かあるいは0であるかを検出する。両方の値がすべて同じでない場合、より多くのビット値を示す側の値とする。以上の処理の埋め込みパターンでは、できるだけ高い密度で埋め込んでいるのでわずかなフレームで電子透かし情報が解読できる。また、長周期的に1ビットずつ検出するため、少しの電子透かしを改ざんしても多数決判定することで求める事ができる。そして、各ビットの判定を埋め込みパターン分判定することで埋め込みパターンを求めることができる。したがって、短周期で埋め込

んだ場合、映像中の数フレーム毎に埋め込み情報があるため、映像データを編集されたりしても検出できるが一方でフレームを抜き取るなどの改ざんに弱い。一方、長周期に埋め込んだ場合、長い期間の映像データを検出しないと埋め込みパターンが検出できないがフレームを抜き取るなどの攻撃に強いため、2つの埋め込みパターンを併用することで弱点を補いあった改ざんや編集につよい埋め込み方法が実現できる。なお、長周期と短周期の併用しかたであるが本実施例以外のやり方でも同様の効果が期待できる。たとえば、1フレームに4ビット埋め込むとしてそのうち3ビットを短周期の埋め込み様に1ビットを長周期の埋め込み様に用いて両方を並列に埋め込むことも出来る。

【0033】

以上示したように本実施の形態のデータ再生装置によれば、鍵記憶装置にその鍵への読み取り履歴を記録しているため、有効期限確認等で現在の時刻を偽って申告しようと試みた場合でもかならず時計を進める方向にしか鍵を受け取れる時刻はないので不正が出来たとしても高々常に再生しつづけた場合に再生できる再生時間以上に再生させることが出来ない様に出来る。また、鍵記憶装置の履歴記録部分の容量は有限なので、履歴容量を越えて鍵を取得することはできないので不正回数の上限を制限できる。

【0034】

また、履歴についてもハッシュ値をつけることにより改ざんが困難な履歴書き込みが実現できる。

【0035】

さらに、本実施の形態によれば、鍵記憶装置に記録した履歴で埋め込みデータの検出精度をあげることが出来るし、また、埋め込み情報で検出した結果との照合は、より確かな不正の証拠を示すことが出来る。

【0036】

さらに情報埋め込みパターンとして短周期と長周期に2つの方法を併用して埋め込むため、改ざんにつよい埋め込み方法が実現できる。

【0037】

なお、鍵記憶手段が鍵の読み出しの際、鍵の有効期間などのチェックを行った

が、データ再生装置が耐タンパ性が保証されていて改造されないのであれば、鍵記憶装置から鍵情報や履歴情報を暗号通信で受け取り、それに基づきデータ再生装置側で判定させる構成を撮ることも出来る。この場合は、履歴情報もデータ再生装置側で作成し鍵記憶装置に暗号通信して記録させることもできる。

【 0 0 3 8 】

また、図 4 の前回アクセス時刻チェックにおいて、履歴情報から時刻情報 w お取り出す際、図 5 のハッシュ値を用いて履歴データ自身が改ざんされていないかどうか確認させるとより安全性が向上する。すなわち履歴情報中からハッシュ値を計算した場合と同じ処理をしてハッシュ値との一致を調べることで改ざんチェックが実現できる。

【 0 0 3 9 】

また、本実施の形態では、履歴に際して鍵の取得時の時刻、終了時の時刻、不使用の時刻と完全に連続した履歴を記録したが、単に、鍵へのアクセス時刻のみを記録しても時計を進ませる方向にしか動かせられない特徴はまた維持でき、本発明の効果を維持しているものである。

【 0 0 4 0 】

【発明の効果】

以上のように本発明（請求項 1）によれば、有効期限付きの鍵についてその申告時刻を逆進させる不正を防止できる。

【 0 0 4 1 】

以上のように本発明（請求項 2、1 0）によれば、鍵取得履歴を改ざんするのが艱難な記録ができる。

【 0 0 4 2 】

また、以上のように本発明（請求項 3）によれば、履歴情報の改ざんによる鍵の有効期間を越え不正使用を防止できる。

【 0 0 4 3 】

また、以上のように本発明（請求項 4）によれば、鍵へのアクセスの上限値を制限できる。

【 0 0 4 4 】

また、以上のように本発明（請求項 5、6、7、8、9）によれば、記録された履歴情報と透かし情報を突き合わせることができるため、不正者への追跡制をより高くすることが出来る。

【0 0 4 5】

また、以上のように本発明（請求項 1 1、1 2）によれば、改ざんに強い透かし埋め込み装置と検出装置が実現できる。

【図面の簡単な説明】

【図 1】

本発明の実施の形態のデータ再生装置および鍵記憶装置を含むシステムの構成図

【図 2】

本発明の実施の形態の鍵記憶装置 2 の構成図

【図 3】

本発明の実施の形態の再生システムの別の構成を示す図

【図 4】

本発明の実施の形態の再生装置鍵取得処理の処理手順の説明図

【図 5】

本発明の実施の形態の履歴情報の記録例の説明図

【図 6】

本発明の実施の形態の記録処理手順の説明図

【図 7】

図 5 のように記録された履歴の電子透かし情報の読み出し処理の説明図

【図 8】

本発明の実施の形態の電子透かし情報埋め込み手段 1 1 あるいは 3 0 8 の構成とその検出装置の構成の説明図

【図 9】

本発明の実施の形態の各フレームに埋め込まれるパターン列を説明する図

【符号の説明】

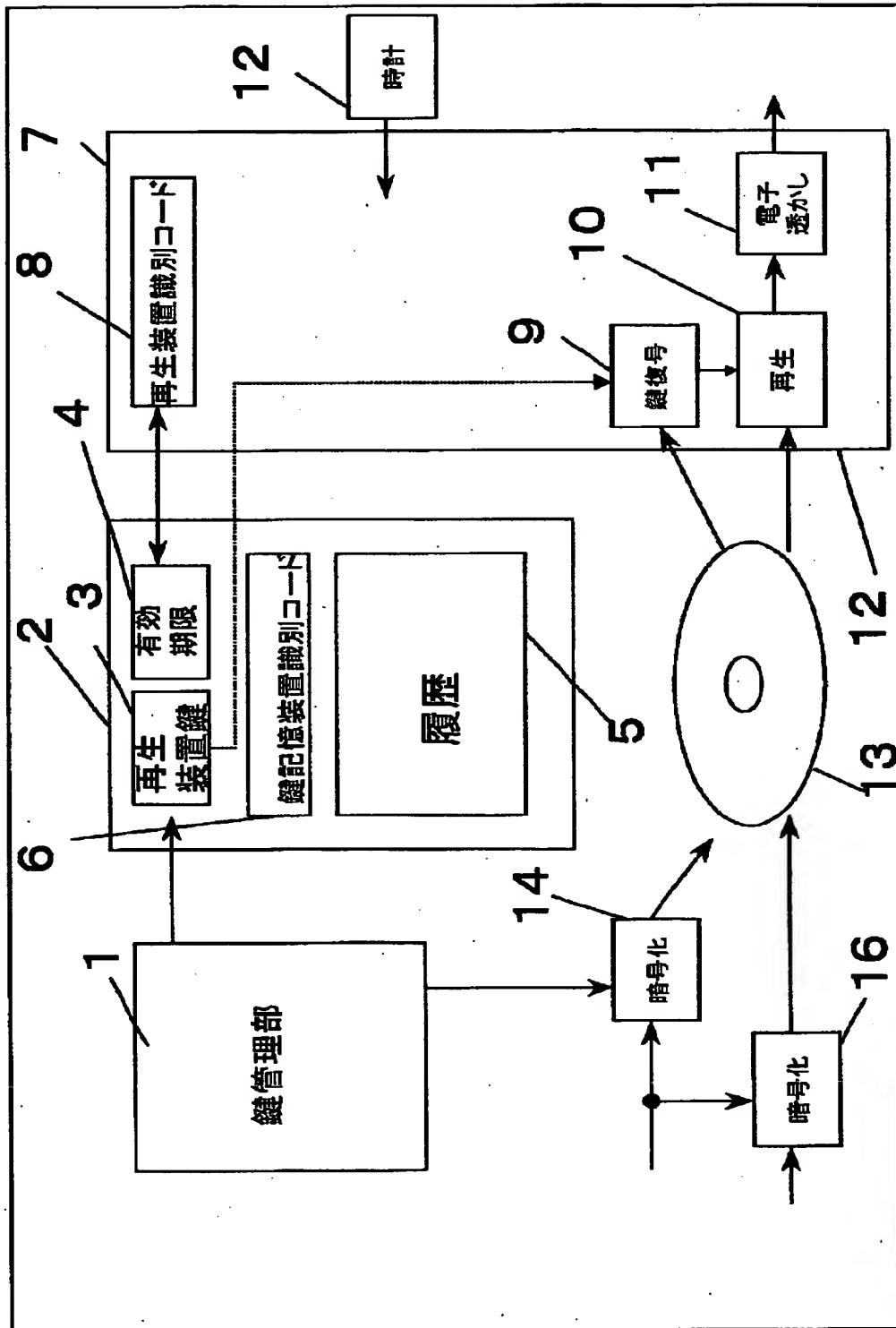
1 鍵管理部

- 2 鍵記憶装置
- 3 再生装置鍵記憶部
- 4 有効期間記憶部
- 5 履歴記憶部
- 6 鍵記憶装置識別コード記憶手段
- 7 データ再生装置
- 8 データ再生装置識別コード記憶部
- 9 鍵複号処理部
- 1 0 再生処理部
- 1 1 電子透かし埋め込み処理部
- 1 2 時計
- 1 3 記録メディア
- 1 4 鍵暗号化手段
- 1 5 情報埋込装置
- 2 0 1 入出力インターフェイス
- 2 0 2 制御部
- 2 0 3 履歴情報記憶部
- 2 0 4 再生装置鍵記憶部
- 2 0 5 有効期間記憶部
- 2 0 6 鍵記憶部再生装置間鍵記憶部
- 2 0 7 鍵記憶装置識別コード記憶部
- 2 0 8 コンテンツ識別コード記憶部
- 2 0 9 再生装置識別コード記憶部
- 2 1 0 時刻情報記憶部
- 3 0 1 入出力インターフェイス部
- 3 0 2 制御部
- 3 0 3 鍵記憶装置識別コード記憶部
- 3 0 4 再生装置識別コード記憶部
- 3 0 5 鍵取得時刻記憶部

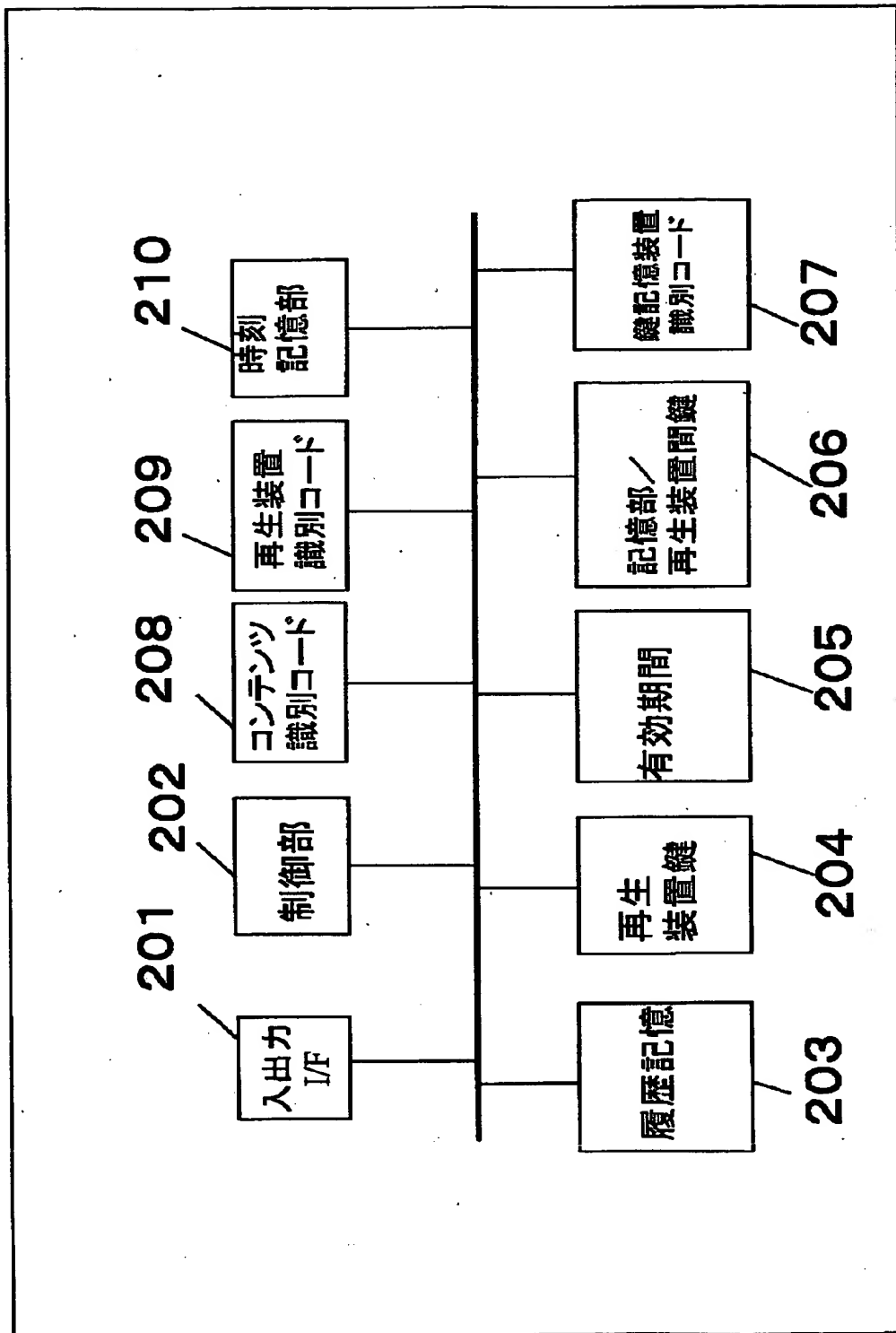
- 3 0 6 鍵復号処理部
- 3 0 7 再生処理部
- 3 0 8 電子透かし情報埋め込み処理部
- 3 0 9 コンテンツ識別コード記憶部
- 3 1 0 鍵記憶部再生装置間鍵記憶部
- 4 0 1 コンテンツ識別コード取得処理
- 4 0 2 時刻情報取得処理
- 4 0 3 鍵リクエスト送信処理
- 4 0 4 最新読み取り時刻との比較処理
- 4 0 5 鍵有効期間確認処理
- 4 0 6 履歴書き込み処理
- 4 0 7 鍵配送処理
- 6 0 1 開始処理
- 6 0 2 未使用期間記録処理
- 6 0 3 開始時刻記録処理
- 6 0 4 鍵使用終了時刻記録処理
- 7 0 1 不正に複製された記録メディア
- 7 0 2 電子透かし情報検出装置
- 7 0 3 再生装置識別コードによる検索検証処理
- 7 0 4 鍵記憶装置識別コードによる検証処理
- 7 0 5 鍵取得時刻情報による検証処理
- 8 0 1 埋め込みシーケンス生成部
- 8 0 2 映像1フレームに情報埋め込み処理する電子透かし埋め込み処理部
- 8 0 3 短周期埋め込みパターン検出部
- 8 0 4 長周期埋め込みパターン検出部
- 8 0 5 電子透かし検出部

【書類名】 図面

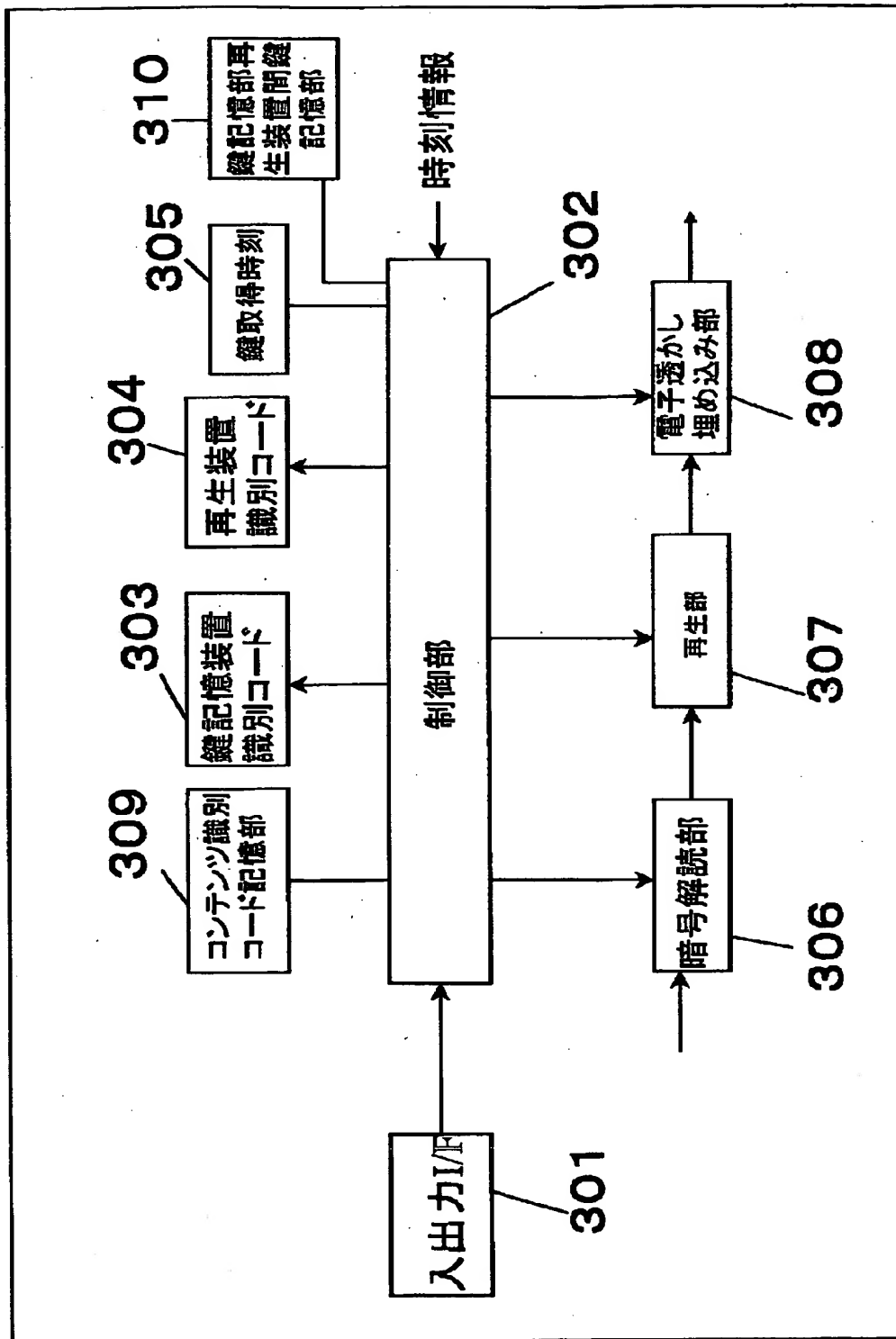
【図 1】



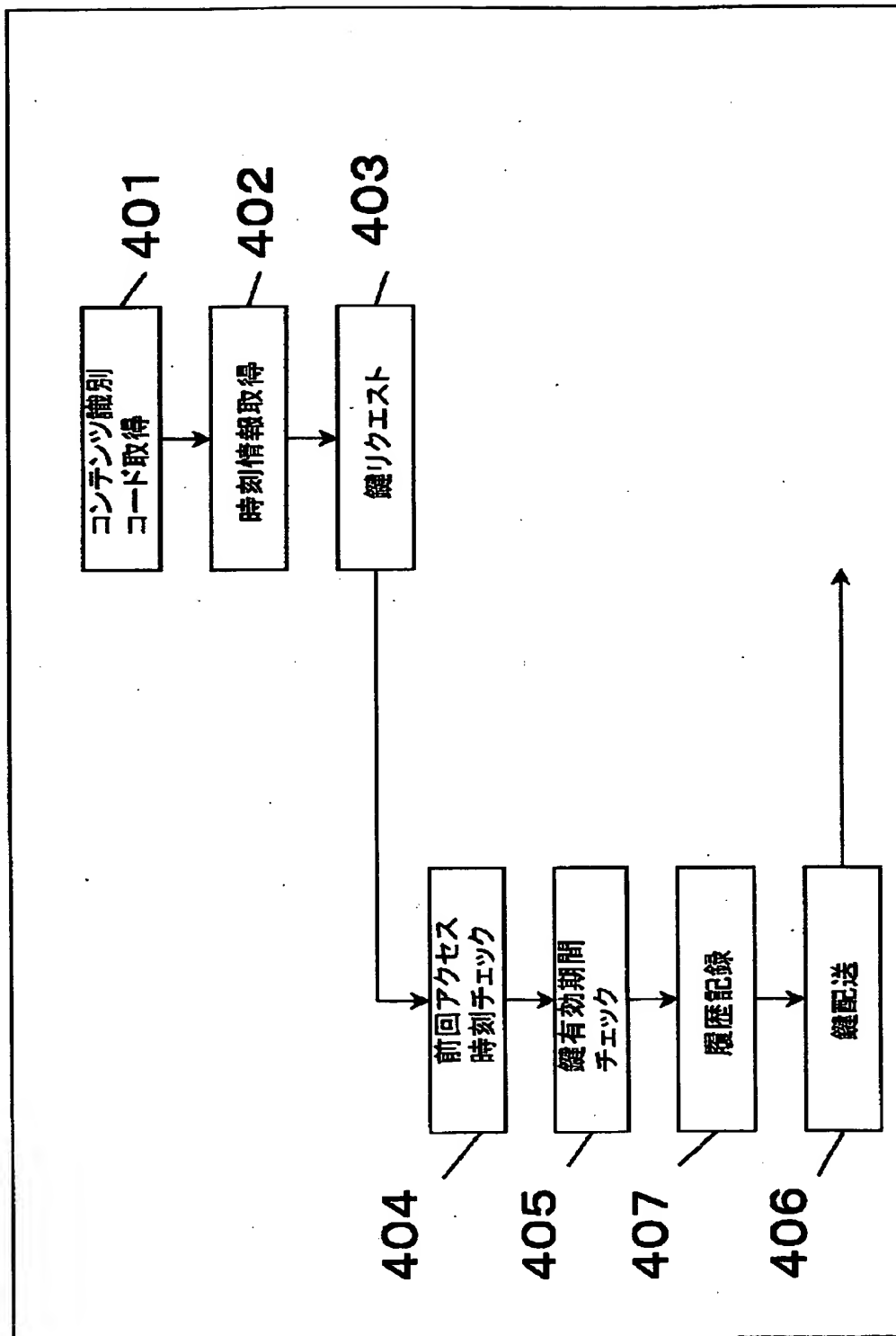
【図 2】



【図 3】



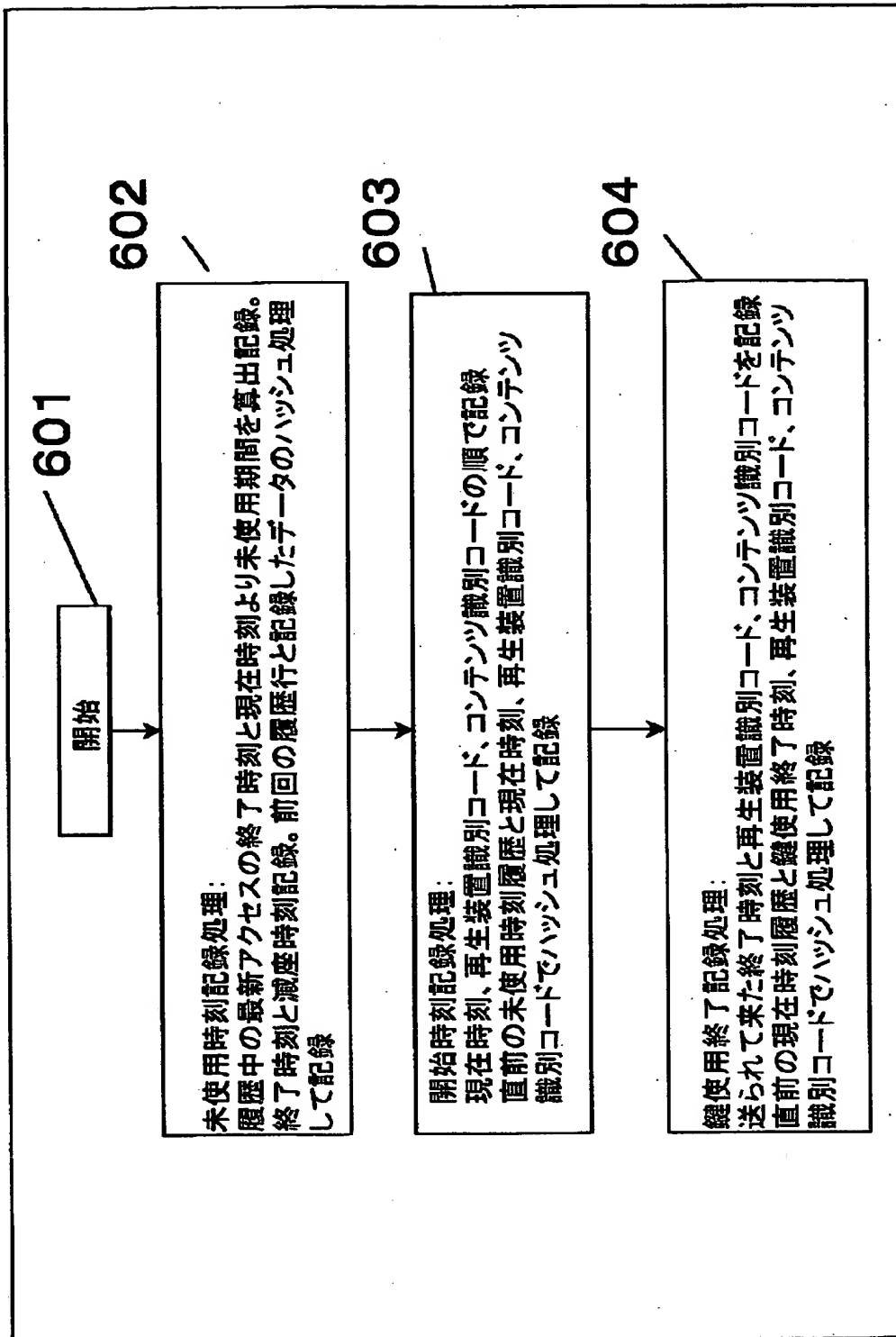
【図 4】



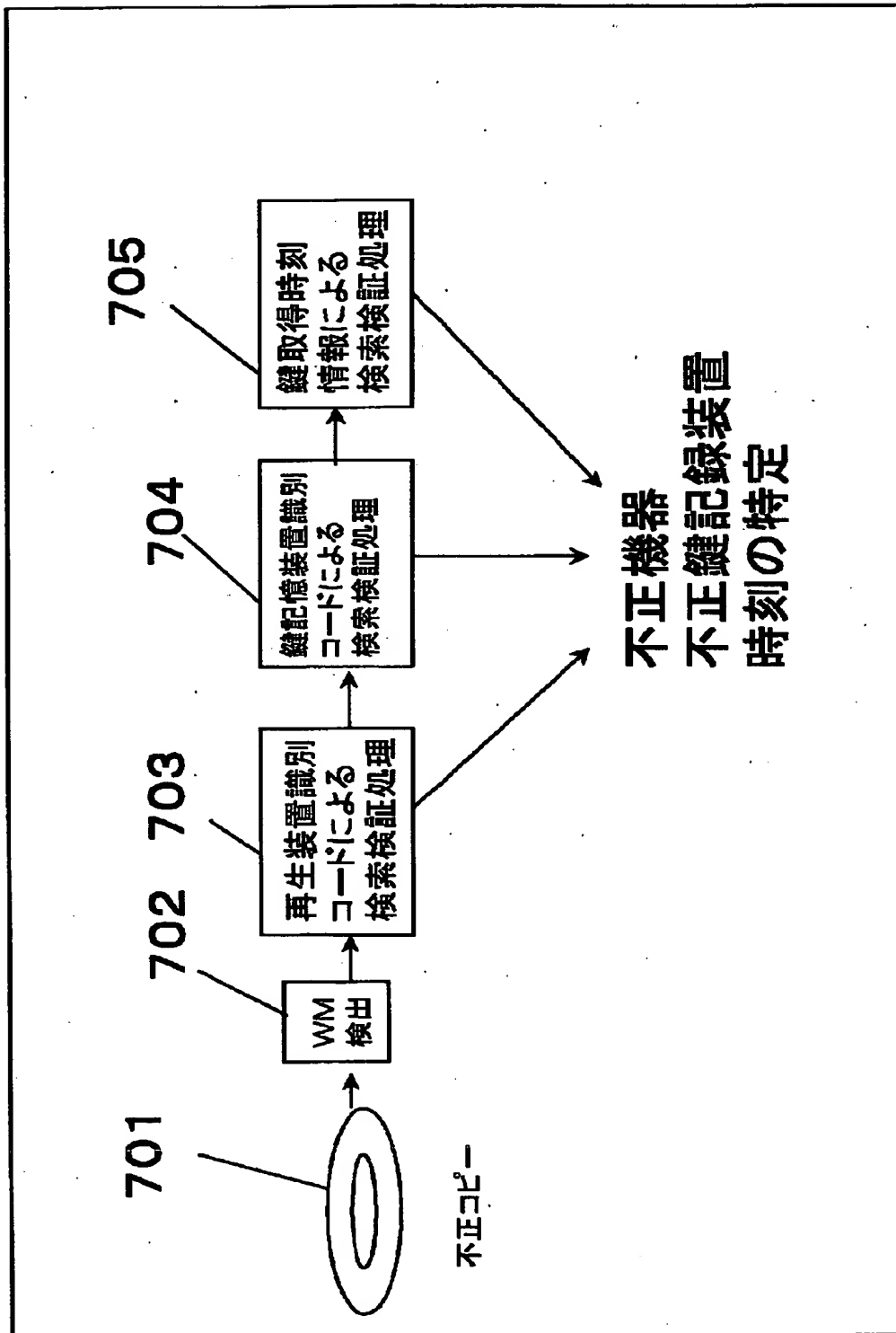
【図 5】

鍵有効時刻			ハッシュ値1
未使用期間	鍵有効時刻	開始時刻1	ハッシュ値2
開始時刻1	再生装置識別コード1	コンテンツ識別コード1	ハッシュ値3
終了時刻1	再生装置識別コード1	コンテンツ識別コード1	ハッシュ値4
未使用期間	終了時刻1	開始時刻2	ハッシュ値5
開始時刻2	再生装置識別コード1	コンテンツ識別コード2	ハッシュ値6
終了時刻	再生装置識別コード2	コンテンツ識別コード2	ハッシュ値7

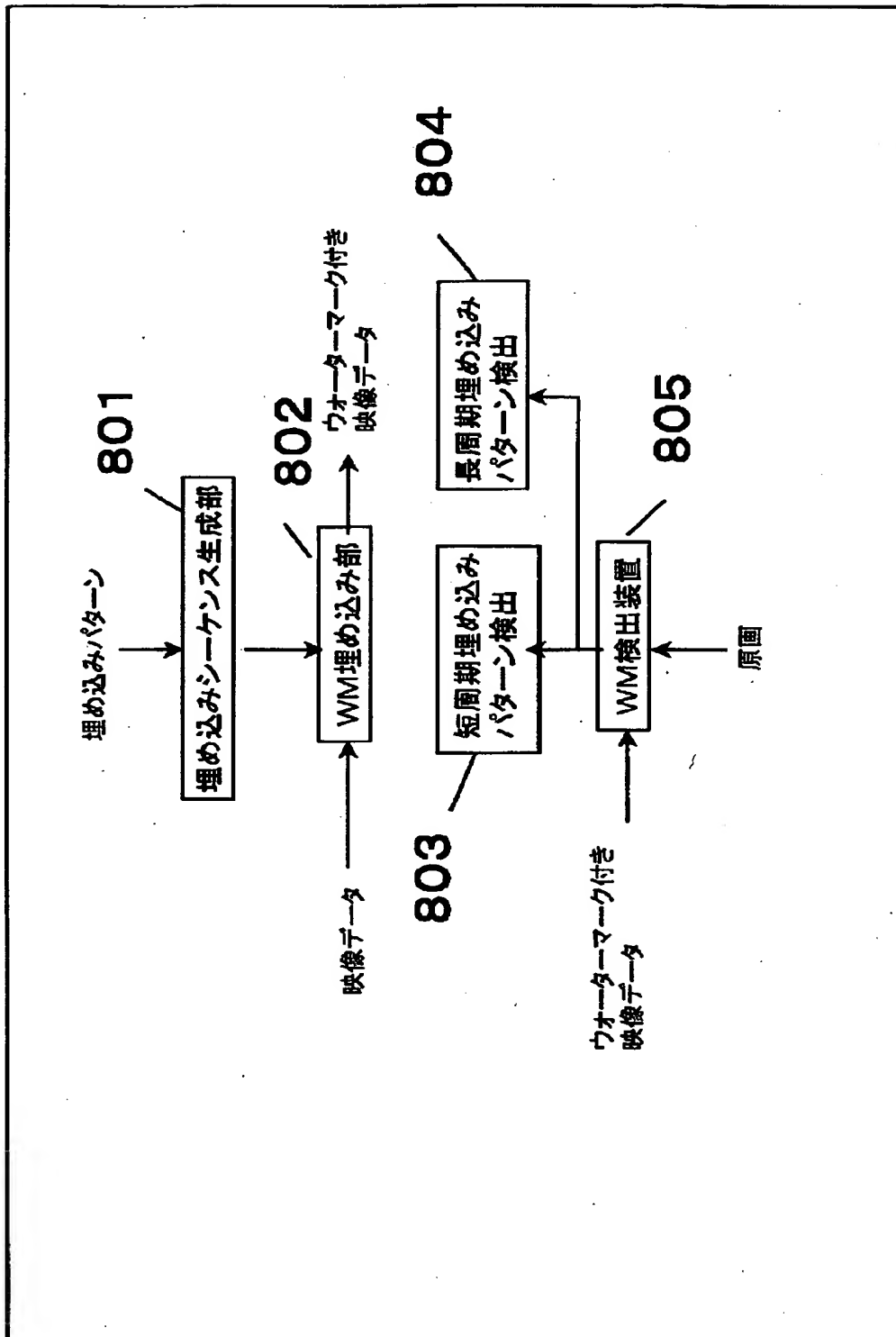
【図 6】



【図 7】



【図 8】



【図 9】

6 5 C a
埋め込みパターン 0110 0101 1100 1010

フレーム番号 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16

6	5	C	a	0	0	0	0	6	5	C	a	F	F	F	F
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

6	5	C	a	F	F	F	F	6	5	C	a	0	0	0	0
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

...

【書類名】 要約書

【要約】

【課題】 再生限定するコンテンツ再生において有効期限付きで再生をするときの時刻情報の改ざんの防止と不正機器の精度の高い追跡性を実現する。

【解決手段】 再生用の鍵を運ぶ鍵記憶手段 2 に鍵へのアクセス履歴を記録していき、再生毎にその時刻と機器からの時刻を比較する。また、透かし情報と履歴情報を比較して追跡性を高める。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社